M系列に基づく一様乱数の生成法 (乱数プログラム・パッケージ)

AUTHOR(S):

伏見, 正則

CITATION:

伏見, 正則. M系列に基づく一様乱数の生成法(乱数プログラム・パッケージ). 数理解析研究所講究録 1983, 498: 99-117

ISSUE DATE:

1983-09

URL:

http://hdl.handle.net/2433/103635

数理解析研究所講究録
498巻 1983年 99-117

M系列に基づく一様乱数の生成法

東大工学部　伏見正則 (Masanori Fushimi)

1. はじめに

M系列を用いて生成される一様乱数列の1周期分に関する基本的な性質——k次均等分布と自己相関関数——について述べる.

M系列

f を GF(2) 上の p 次の原始多項式, D を"添字を1減らす演算子"とするとき, 差分方程式

$$f(D)a_t = 0 \pmod 2 \tag{1}$$

を

$$(a_0, a_1, \cdots, a_{p-1}) = (0, 0, \cdots, 0) \tag{2}$$

以外の任意の初期条件の下に解いて得られる系列 $\{a_t\}$ のことを, f を特性多項式とするM系列と呼ぶ。$\{a_t\}$ は周期列であり, その周期 T は

$$T = 2^p - 1 \tag{3}$$

で与えられる.

M系列を基にして, 次のようなlビットの2進小数の系列を構成する.

横型系列 $\{x_t\}$:

$$x_t = 0.a_{\sigma t}\, a_{\sigma t+1} \cdots a_{\sigma t+l-1}, \qquad \gcd(\sigma, T)=1 \tag{4}$$

縦型系列 $\{y_t\}$:

$$y_t = 0.a_{t+\tau_1}\, a_{t+\tau_2} \cdots a_{t+\tau_l} \tag{5}$$

横型系列はTausworthe [12] の提案したものであり, 縦型系列はLewis & Payne [10]の提案したものの一般化になっている. (Lewis & Payneの提案では, fとして3項式を使っているが, ここではその制約はおかない. また彼等の方法では, $\tau_1, \tau_2, \cdots, \tau_l$ は任意でよいのか, $\tau_2-\tau_1 = \tau_3-\tau_2 = \cdots = \tau_l-\tau_{l-1}$ でなければならないのかが不明確であるが, ここではごく一般的な形にしておく.)

k次均等分布

lビットの2進小数値を取る確率変数の列 $\{X_t\}$ が, すべてのlビットの2進小数のk個組 $(v_1, v_2, \cdots, v_k)$ に対して

$$\Pr\{(X_t, X_{t+1}, \cdots, X_{t+k-1}) = (v_1, v_2, \cdots, v_k)\} = \frac{1}{2^{kl}} \tag{6}$$

を満たすとき, $\{X_t\}$ はk次均等分布をするという. また, mを自然数とするとき, すべての整数j $(0 \le j < m)$ に対

して

$$Pr\{(X_{mt+j}, X_{mt+j+1}, \cdots, X_{mt+j+k-1}) = (v_1, v_2, \cdots, v_k)\} = \frac{1}{2^{kl}} \qquad (7)$$

が成立するとき，$\{X_t\}$ は (m, k) 均等分布をするという．

擬似乱数列は確率変数列ではないので，(6)，(7) の左辺の $Pr\{\cdot\}$ は，相対頻度の極限＝1周期分の相対頻度の意味に解釈することにする．またM系列の基本的な性質――相続く p 個組を1周期分について見ると，“p 個とも0”を除くすべてのパターンが1回ずつ出現する――により，$v_1 = v_2 = \cdots = v_k = 0$ の場合の頻度は，その他の場合の頻度に比べて1だけ少ない．したがって (6)，(7) の等号は厳密には成立し得ないが，2^{-p} 程度のくい違いを許容することにすれば，成立し得ることになる．そこで，以後均等分布という用語はこのくい違いを許容した意味で用いることにする．また，$\{x_t\}$ あるいは $\{y_t\}$ が k 次均等分布をしている場合に，それらが (m, k) 均等分布をするための必要十分条件は，m が T と互いに素であることであるが，以後は k 次均等分布の条件だけを考察の対象とする．

k 次均等分布の概念は，統計的検定法のひとつである系列検定（*serial test*）と密接に関連している．ある数列が1次元の度数検定に合格したとしても，それによって（ある数

値の次に特定の数が出やすいという傾向が無いという意味での）ランダムネスまでも保証されるわけではない。そこで，ランダムネスをチェックするために（2次の）系列検定（＝2次元の度数検定）が行われる。さらに念入りにランダムネスをチェックするためには，3個組，4個組，… に対する系列検定（＝3次元，4次元，… の度数検定）を行う必要がある。また，数列を基にして2次元のランダムな点列を発生させようとする場合には，2次の系列検定は単に度数の一様性をチェックするだけであるから，ランダムネスを保証するためには，最低限4次の系列検定を行わなければならないことになる。しかしながら，系列検定の次数を上げると計算量が急激に増大するので，通常は高次の検定は行わずに，ポーカー検定等の分類の粗い検定で代用している。k次均等分布をする系列を作ることは，1周期全体についてはk次の系列検定に合格する系列を作ることに他ならず，したがってkの値は大きいことが望ましいと考えられる。

<u>自己相関関数</u>

$\{x_t\}$ の1周期全体にわたる平均値を $\bar{x}$ とすると，この系列の自己相関関数は

$$R_x(\delta) = \frac{1}{T}\sum_{t=1}^{T}(x_t-\bar{x})(x_{t+\delta}-\bar{x}) \qquad (8)$$

によって定義される．$\{y_t\}$ の自己相関関数 $R_y(\delta)$ につい

ても同様である。これらの値は，λの値がなるべく大きいところまでほぼ0に等しいことが望ましい。

2. 横型系列の性質

横型系列の性質はTausworthe [12]によって解明されている。その主要結果を示せば次のとおりである。

定理1. $\sigma \geq l$とする。このとき，$\{x_t\}$は$k \leq \lfloor p/\sigma \rfloor$の範囲の$k$について$k$次均等分布をする。また，$1 \leq \lambda \leq (T-l)/\sigma$ならば$R_x(\lambda) \fallingdotseq 0$である。

この定理で述べられていることだけから判断すれば，$\sigma = l$と選ぶのがよく，このとき達成できる均等分布の最大の次元$\lfloor p/l \rfloor$は，M系列に基づくlビットのあらゆる一様乱数列（横型，縦型を問わない）が達成できる均等分布の最大の次元になっている。しかし，σをlより大きくとることによって，別の観点から見て好ましい乱数列が得られる場合があることを注意しておこう。[14]（上の定理は，$\lfloor p/\sigma \rfloor$より高次の均等分布は達成できないとは主張していないことに注意する必要がある。）

3. 縦型系列の性質

特性多項式として3項式

$$f(D) = D^p + D^q + 1 \qquad (9)$$

を用いる縦型系列は，初めLewis & Payneによって提案された。彼等の方法は，乱数発生の段階では速いが，①初期値設定に手間がかかり，②多次元の均等分布の理論的保証がないという欠点を持つ。①の欠点を除く試みはArvillias & Maritsas [1], Payne & McMillen [11]等によって行われたが，いずれも②の欠点には気付いていない。そこで，ここでは主として②およびその対策について述べる。（①の対策については4節で述べる。）

特性多項式として(9)を用いる場合には，$\{y_t\}$は漸化式

$$y_t = y_{t-p} \oplus y_{t-q} \qquad (10)$$

によって生成される。ここに，⊕は排他的論理和（exclusive or）を表わし，たいていの計算機で高速に処理できる演算である。この漸化式によって$\{y_t\}$を生成するためには，初期値$y_0, y_1, \cdots, y_{p-1}$を与える必要がある。$y_t$ $(0 \le t \le p-1)$を（2進数としてではなくて）l個のビットの並び，すなわち成分がすべて0か1かSなるl次元の行ベクトルと見なして，第$t+1$行に配置して得られるp行l列の行列$S(y)$のことを，系列$\{y_t\}$の初期行列（seed matrix）と呼ぶ。

Lewis & Payne は初期値の設定の仕方として次のような提案をした。

① $S(y)$ の列ベクトルが1次独立となるようにする。

そのためには、

② ビット間の位相差 $\tau_j - \tau_{j-1}$ $(j=2,3,\cdots,l)$ がすべて等しく、その値でがM系列の周期Tと互いに素であるようにするとよい。

しかしながら、この条件は、発生される系列 $\{y_k\}$ が1次均等分布をすることを保証するだけであって、よい乱数列が発生されることを保証するものではないことに注意する必要がある。実際、図1は、521次の原始3項式を用いて、Arvillias & Maritsas の Fig. 3 に示されている方法によって発生された系列を使って作った2次元点列を示したものであるが、ランダムな点列とはかけ離れた様相を示している。彼等の方法に対する初期行列 $S(y)$ の行ベクトルが1次独立であることを示すことは可能ではあるが、類似の構造をもった、もっと周期の短い系列を考察する方が簡単で、ことの本質を理解しやすいので、そうすることにする。

図2は、$f(D)=D^7+D^4+1$, $a_0=a_1=\cdots=a_6=1$, $l=3$, $\tau\,(=\tau_2-\tau_1=\tau_3-\tau_2)=96$, として得られる系列 $\{y_k\}$ の1周期分を示したものである。この初期行列 $S(y)$

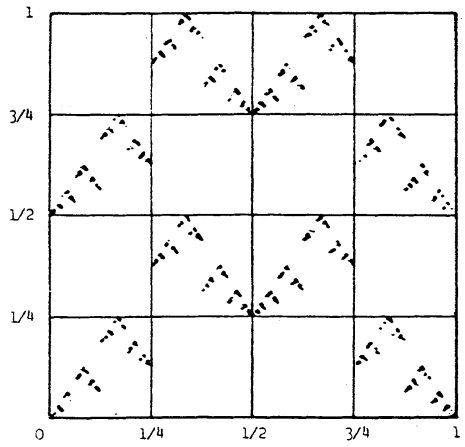

図1. 2次元分布が均等でない例.

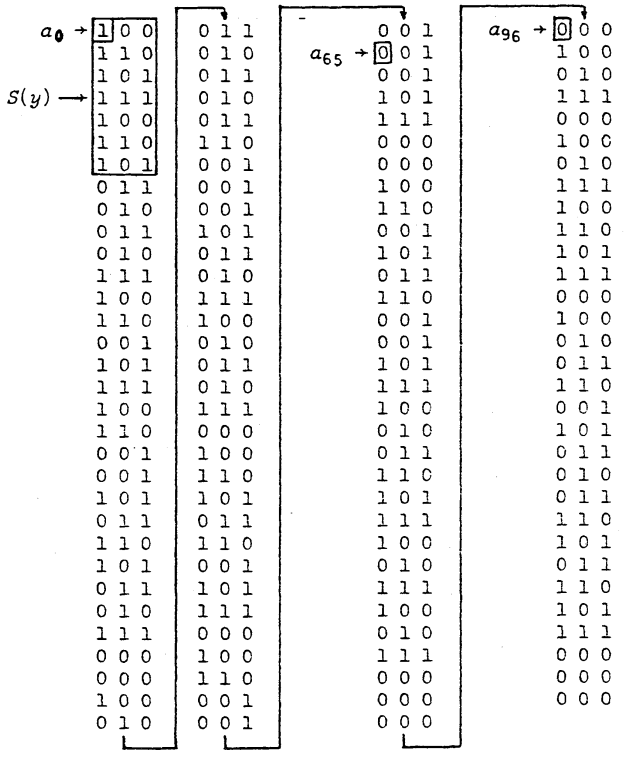

図2. $f(D)=D^7+D^4+1$, $\tau=96$, $l=3$ として得られる縦型系列.

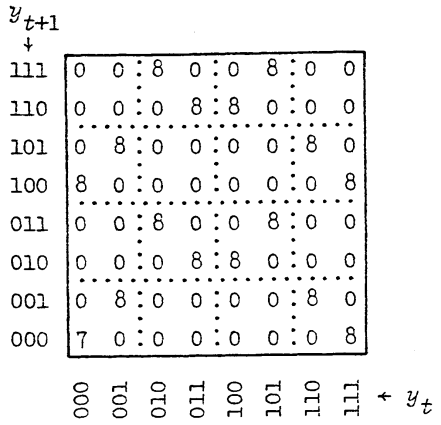

図3. 図2の例の2次元分布.

の列ベクトルが1次独立であることは容易にわかる。しかしながら，図3に示すとおり，この系列の2次元分布は均等分布ではない。（$\lfloor p/l \rfloor = 2$ であるから，2次の均等分布は達成可能なものであることに注意。）この系列が2次均等分布を達成できない理由は次のとおりである。すべての a_t $(t \geq 7)$ は $a_0, a_1, \cdots, a_6$ で表現できる。実際 $a_{96} = a_3 + a_4 +$

$a_5 + a_6$ ($\mathrm{mod}\ 2$, 以下略), $a_{97} = a_0 + a_3 + a_4 + a_5 + a_6$, $\cdots$; $a_{65} = a_3 + a_5$, $a_{66} = a_4 + a_6$, $\cdots$ 等であり, これから, $a_0 + a_{96} = a_{97}$, $a_1 + a_{97} = a_{98}$, $\cdots$; $a_{96} + a_{65} = a_{66}$, $a_{97} + a_{66} = a_{67}$, $\cdots$ 等が導かれる。すなわち, y_{t+1} の2番目(3番目)のビットは, y_t の1番目と2番目(2番目と3番目)のビットの和として求められることになる。したがって $\{(y_t, y_{t+1})\}$ という系列を考えると, けっして現われないパターンがあることになる。これが図3に度数が0のパターンがたくさんある理由である。

この例から, 一般に l ビットの系列 $\{y_t\}$ が k 次均等分布をすることを保証するためには, 初期行列 $S(y)$ の l 列の1次独立性ではなくて, $S(y)$ の相続く k 行からなる小行列のすべての要素 kl 個の独立性を考えなければならないことがわかる。そして, 実際, 次の定理が成立する[6]。

定理2. 縦型系列 $\{y_t\}$ が k 次均等分布をするための必要十分条件は, この系列の相続く k 個の要素を構成するM系列の kl 個の要素が1次独立であることである。また, $1 \leq \Delta \leq \min_{i \neq j} |\tau_i - \tau_j|$ ならば $R_y(\Delta) \fallingdotseq 0$ である。

この定理を用いると, ① $\{y_t\}$ が k 次均等分布をするように $S(y)$ を設定するアルゴリズムを設計すること, および

② $S(y)$ または $(\tau_1, \tau_2, \cdots, \tau_l)$ が与えられたときに，それによって生成される系列 $\{y_t\}$ が k 次均等分布をするかどうかを理論的に検定することができる．これらの詳細については［6］を参照されたい．

4. 横型系列と縦型系列の関係

この節では，隣接するビット間の位相差が一定：

$$\tau_j - \tau_{j-1} = \tau \quad (j = 2, 3, \cdots, l), \quad \gcd(\tau, T) = 1 \tag{11}$$

という制約を課して得られる縦型系列の全体と，横型系列の全体との対応関係を考える．横型系列および縦型系列を構成するM系列の特性多項式およびパラメタを明示するために，以後必要に応じて $\{x_t(f;\sigma)\}$，$\{y_t(f;\tau)\}$ と書くことにする．

まず，準備のために，有限体の理論で知られているいくつかの事実を述べよう．1以上で T 未満の整数のうちで T と互いに素なもの（$\varphi(T)$ 個ある）の全体を R とする．R は T を法とする乗法に関して群をなす．集合

$$C_0 = \{1, 2, 4, \cdots, 2^{p-1}\}$$

は，正規部分群であり，その剰余類は（C_0 も含めて）$K \equiv \varphi(T)/p$ 個ある．それらを (C_0)，C_1，C_2，$\cdots$，C_{K-1} で表わすことにする．次に，$\{a_t\}$ がM系列であるとすると，

これから $r(\in R)$番目ごとの要素を系統的にサンプリングして得られる系列 $\{a_{rt}\}$ もM系列である。$r_1, r_2 \in R$ とすると，二つのM系列 $\{a_{r_1 t}\}$, $\{a_{r_2 t}\}$ は，r_1 と r_2 が同一の剰余類に属するとき，かつその時に限り，同一の原始多項式を特性多項式とする。そこで $\{a_t\}$ に対応する原始多項式 f を f_0 と書くことにし，$C_1, C_2, \cdots, C_{K-1}$ に属する r に対応するM系列 $\{a_{rt}\}$ を生成する原始多項式を $f_1, f_2, \cdots, f_{K-1}$ と書くことにする。

定理3. 任意の p と l $(2 \le l \le p)$ に対して次の命題が成り立つ。

縦型系列（横型系列）の中で，位相をずらせても重なり合わないという意味で本質的に異なるものの個数は $\varphi^2(T)/p$ 個である。一方の型の任意の系列に対して，これと本質的に同じ他方の型の系列がひとつ存在する。対応関係は次のとおりである。

$$\{x_t(f_0;\sigma)\} \simeq \{y_t(f_i;\sigma^{-1})\} \quad \text{if } \sigma \in C_i \tag{12}$$

$$\{y_t(f_0;\tau)\} \simeq \{x_t(f_j;\tau^{-1})\} \quad \text{if } \tau \in C_j \tag{13}$$

ここに，σ^{-1}, τ^{-1} は群Rにおける σ, τ の逆元を表わし，記号 $\simeq$ は両辺の系列が位相を適当にずらせば一致することを表わす。

応用

この定理を用いると，Lewis & Payne の方法のもつ二つの欠点（6ページ）を除くことができる。簡単のために，乱数のビット数 l が2のべき乗である場合の方法について述べるが，そうでない場合にも簡単な修正で適用できる。$l=2^d$ とし，$\tau = 2^p/l \in C_0$ と選ぶ。そうすると $\tau^{-1}=l$ であるから，定理により

$$\{y_t(f_0;\tau)\} \simeq \{x_t(f_0;l)\}$$

が得られる。したがって，M系列の最初の lp 個の要素 a_t $(0 \le t \le lp-1)$ を（$\sigma=l$ として）横型に並べれば，縦型系列 $\{y_t(f_0;\tau)\}$ の初期値の設定が完了することになる。

一例として，$f(D)=D^{521}+D^{32}+1$，$l=32$ の場合の整数の縦型系列 $\{Y_t\}=\{2^l y_t\}$ の初期値の設定方法を示そう。

手順1．32ビットの2進整数 Y_t $(0 \le t \le 16)$ を任意に与える。（ただし $Y_0, \cdots, Y_{15}$ の全ビットおよび Y_{16} の下位9ビットのすべてが0とはならないようにする。）

手順2．Y_{16} を次式により更新する。

$$Y_{16} = M^{32}((L^{23}Y_{16} + R^9 Y_0) \oplus Y_{15})$$

手順3．漸化式

$$Y_t = M^{32}((L^{23}Y_{t-17} + R^9 Y_{t-16}) \oplus Y_{t-1})$$

を用いて Y_t ($17 \leq t \leq 520$) を求める。

この手順中の＋は論理和，⊕は排他的論理和，L^{23} は 23 ビット左論理シフト，R^9 は 9 ビット右論理シフト，M^{32} は下位 32 ビットを取り出すマスク演算を表わす。（1語が 32 ビットの計算機を用いるなら，マスク演算はもちろん不要である。）また，手順1で初期値を与える部分は，例えば合同法乱数などを使ってランダムに設定するのがよい。0あるいは1が極端に多いビット列を与えると，その後に続くM系列の部分列は，かなり長い間にわたって性質がよくないことが多いことが経験的に知られている。

定理3の他の応用としては，相互相関の無い複数の乱数列の発生算法の設計[4]，横型系列について得られている結果（例えば[13]）の縦型系列への翻訳などがあるが，ここでは割愛する。

5. 上位ビットの高次均等分布を保証する方法

Tootill 等[14] は，均等分布の観点から見て大変に好ましいひとつの系列を発見している。それは，$f(D)=D^{607}+D^{273}+1$，$r=512$，$l=23$ として得られる横型系列で，次の特長を持っている。

すべての l' ($1 \leq l' \leq l$) について性質Pが成り立つ。

性質P: 上位の l' ビットを読み出して得られる系列は

$\lfloor P/l' \rfloor$ 次均等分布をする。

彼等はこの系列を試行錯誤によって求めたのであるが，同じ性質を持つ他の系列をやはり試行錯誤によって探すのは大変である。しかし，条件を少し弱めて，“l' が2のべき乗である限り性質Pが成り立つ”系列ならば，次のようにすれば簡単に作れる。

この方法の基本的な考え方は，横型系列のビットの位置を入れ替えることである。入れ替えの操作を実際に行なうのは初期行列を作成する段階だけであり，乱数列発生の段階では，縦型系列と見なして漸化式（3項式の場合には(10)式）を用いて生成すればよいので，余計な手間はかからない。

まず自然数 i に対して

$$e(i) = \text{“}i\text{以上で最小の2のべき乗数”}, \tag{14}$$

$$\pi(i) = (2i-1)\,e(l)/e(i) - e(l) \tag{15}$$

と定義する。（一例として，表1に，$16 < l \leq 32$ の場合の $e(\cdot)$ と $\pi(\cdot)$ を示した。）$\pi(\cdot)$ を用いて，$\{x_t\}$ のビットの位置を入れ替えた系列 $\{x'_t\}$ を次式により定義する。

$$x'_t = 0.a_{ot+\pi(1)}\,a_{ot+\pi(2)}\cdots a_{ot+\pi(l)} \tag{16}$$

このとき，次の定理が成立する。

表1. $16 < l \leq 32$ の場合の $e(\cdot)$ と $\pi(\cdot)$

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	...	32
π(i)	0	16	8	24	4	12	20	28	2	6	10	14	18	22	26	30	1	3	5	...	31
e(i)	1	2	4	4	8	8	8	8	16	16	16	16	16	16	16	16	32	32	32	...	32

定理4. $\sigma = e(l)$ とする。$\{x_t'\}$ の上位の i ビットのみに注目すると，$k \leq \lfloor p/e(i) \rfloor$ の範囲の k 次均等分布が保証される（$1 \leq i \leq l$）.

この定理の証明は，4節で述べたM系列の系統サンプリングの性質を使えば容易にできる。

$f(D)$ が3項式 (9) の場合の $\{x_t'\}$ の初期値設定アルゴリズムを図4に示す。ここで，$S = \sigma = e(l)$ であり，$p[i] = \pi(i)$, $1 \leq i \leq l$, である。また $a[t]$, $0 \leq t \leq p-1$, にはM系列の初期値を入れておく必要がある。なお，プログラム中の $W[t]$ は整数であり，$2^l x_t'$ に相等する。

M系列の初期値，すなわち0と1からなる p 個組をデータとして与えるのは，“自由度が大きすぎて”不便なこともあるであろう。そこで，合同法を用いてこれも計算機内部で設定するFORTRANプログラムの一例を図5に示す。使用している原始多項式は，4節でも例に挙げた $f(D) = D^{521} + D^{32} + 1$ である。想定している計算機は，1語＝32ビットのIBM

```
j:=-1;
for t:=0 to p-1 do
  begin
    for i:=0 to s-1 do
      begin
        j:=mod(j+1,p);  aa[i]:=a[j];
        jq:=mod(j-q,p); a[j]:=mod(a[j]+a[jq],2)
      end i;
    Wt:=0;
    for i:=1 to l do
      Wt:=2*Wt+aa[pi[i]];
    W[t]:=Wt
  end t
```

図4. 3項式に基づく $\{2^l x_i\}$ の初期値設定算法

型のものであり，$l=31$ ビットの非負整数型の乱数列の初期値を設定するようになっている．引数の意味は次のとおりである．

MLTPLY: 乗算型合同法の乗数，

IRND: 同上の初期値，

W: 乱数列の初期値を返す配列．

```
      SUBROUTINE INTLZ(MLTPLY,IRND,W)
      IMPLICIT INTEGER (A-Z)
      DIMENSION W(521),A(521),AA(32)
C     INITIALIZE M-SEQUENCE USING CONGRUENTIAL METHOD
      DO 10 T = 1, 521
      IRND=MLTPLY*IRND
   10 A(T)=ISIGN(1,IRND)
C     INITIALIZE THE 31-BIT INTEGER SEQUENCE
      J=-1
      DO 40 T = 1, 521
      DO 20 I = 1, 32
      J=MOD(J+1,521)
      AA(I)=(A(J+1)-1)/(-2)
      JQ=MOD(J-32,521)
   20 A(J+1)=A(J+1)*A(JQ+1)
      WT=((((((AA(1)*2+AA(17))*2+AA(9))*2+AA(25))*2+AA(5))
     +     *2+AA(13))*2+AA(21))*2+AA(29)
      DO 30 I = 3, 31, 4
   30 WT=WT*2+AA(I)
      DO 35 I = 2, 30, 2
   35 WT=WT*2+AA(I)
   40 W(T)=WT
      RETURN
      END
```

図5. $f(D)=D^{521}+D^{32}+1$ に基づく 31 ビットの整数型乱数列の初期値を設定するプログラム

6. まとめ

M系列を用いて生成される一様乱数列の1周期全体に関する基本的な性質について述べた。これにより，1周期全体に

わたる性質のよい乱数列を高速に発生することが可能になった。

しかしながら，ここで述べたことは，実際に使われる個々の部分列の良さまで保証するものではないことに注意する必要がある。統計的検定は不可欠であろうと思われる。

参考文献

[1] Arvillias, A. C., and Maritsas, D. G. Partitioning the period of m-sequences and application to pseudorandom number generation. J. ACM 25, 675-686 (1978).

[2] Bright, H., and Enison, R. Quasi-random number sequences from a long TLP generator with remarks on application to cryptography. Computing Surveys 11, 357-370 (1979).

[3] Fushimi, M. Increasing the orders of equidistribution of the leading bits of Tausworthe sequence. Information Processing Letters 16, 189-192 (1983).

[4] 伏見正則. M系列に基づく乱数発生法に関する相反定理とその応用. 情報処理学会論文誌に掲載予定 (1983).

[5] 伏見正則，手塚 集. 多次元分布が一様な擬似乱数の生成法，応用統計学 10，151-163 (1981).

[6] Fushimi, M., and Tezuka, S. The k-distribution of the generalized feedback shift register pseudorandom numbers. to appear in Comm. ACM (1983)

[7] 泉 照之，柏木潤. 2値乱数源用高次M系列の初期値.

計測自動制御学会論文集 18, 929-935 (1982).

[8] Golomb, S. W. Shift Register Sequences. Holden-Day, San Francisco, 1967.

[9] Knuth, D. E. The Art of Computer Programming, Vol. 2: Seminumerical Algorithms. 2nd Ed. Addison-Wesely, Reading, Mass. (1981).

[10] Lewis, T. G., and Payne, W. H. Generalized feedback shift register pseudorandom number algorithms. J. ACM 20, 456-468 (1973).

[11] Payne, W. H., and McMillen, K. L. Orderly enumeration of nonsingular binary matrices applied to text encryption. Comm. ACM 21, 259-263 (1978).

[12] Tausworthe, R. C. Random numbers generated by linear recurrence modulo two. Mathematics of Computation 19, 201-209 (1965).

[13] Tootill, J. P. R., Robinson, W. D., and Adams, A. G. The runs up-and-down performance of Tausworthe pseudo-random number generators. J. ACM 18, 381-399 (1971).

[14] Tootill, J. P. R., Robinson, W. D., and Eagle, D. J. An asymptotically random Tausworthe sequence. J. ACM 18, 381-399 (1973).